STATEWIDE INFORMATION SYSTEMS POLICY

Statewide Policy: Computer Virus Detection and Protection

Product ID: ENT-SEC-102

Effective Date: October 2004

Approved: Steve Bender, Acting Director, Department of Administration

Replaces & Supercedes: This policy supercedes any prior enterprise policies for establishing and implementing information technology (IT) policies and standards.

I. Authorizations, Roles, & Responsibilities

Pursuant to the Montana Information Technology Act ("MITA") (Title 2, Chapter 17, Part 5 of the Montana Code Annotated ("MCA"), it is the policy of the state that information technology be used to improve the quality of life of Montana citizens, and that such improvement is to be realized by protecting individual privacy and the privacy of the information contained within the state's information technology systems. §2-17-505(1), MCA. It is also the policy of the state that the development of information technology resources be conducted in an organized, deliberative, and cost-effective manner, which necessitates the development of statewide information technology policies, standards, procedures, and guidelines applicable to all state agencies and others using the state network. It is also anticipated that State information technology systems will be developed in cooperation with the federal government and local governments with the objective of providing seamless access to information and services to the greatest degree possible. §2-17-505(2), MCA.

Department of Administration: Under MITA, the Department of Administration ("DOA") is responsible for carrying out the planning and program responsibilities for information technology for state government (except the national guard), including for establishing and enforcing a state strategic information technology plan and establishing and enforcing statewide information technology policies and standards. DOA is responsible for implementing MITA and all other laws for the use of information technology in state government. The director of DOA has appointed the chief information officer to assist in carrying out the department's information technology duties. §2-17-512, MCA.

Department Heads: Each department head is responsible for ensuring an adequate level of security for all data within their department. §2-15-114, MCA.

II. Policy - Requirements

A. Scope

This policy applies to all computers that reside on the inside of the state's Internet firewall, including all state agencies as well as local government entities. This policy does not apply to colleges and universities, the Commissioner of Higher Education Office, or public access computers in libraries.

B. Purpose

The Department of Administration's Information Technology Services Division (ITSD) is responsible for providing computer security for the Montana state network. To accomplish this, viruses must be kept from infecting the state network

C. Requirements

Each user of the State of Montana's computing and information resources should realize the fundamental importance of information resources and is responsible for the safe keeping of these resources.

Users and network system administrators must guard against viruses that disrupt or threaten the viability of all systems, including those on the State network and those on networks to which State systems are connected. Virus scanning software MUST be installed, updated, and used regularly on servers, workstations, portable computers (such as Personal Digital Assistants [PDAs], smart phones, etc.), and any other computers being used to connect to the state's network remotely.

Users shall not knowingly introduce a computer virus into a state computer. Using the virus scanning software tools installed on the computer, users MUST scan files and software downloaded from the Internet or from any external source, regardless of its origin. Users must scan ALL removable media if it has been used any place other than their own workstation.

Each user is responsible for having knowledge of the State's policies concerning security and care for their computer.

A user that suspects that his/her workstation has been infected by a computer virus must IMMEDIATELY POWER OFF the computer and notify their Network Administrator or designated contact person to coordinate virus removal operations. Much of the damage attributed to viruses occurs through improper removal attempts.

Most computer viruses are introduced via electronic mail. Virus scanning software has been installed on all enterprise email servers. To avoid virus infiltration, filtering mechanisms may be incorporated without prior notification.

Further protections for laptop computers including the installation of a firewall product, have been included in the Workstation, Portable Computer, and PDA Policy, ENT-SEC-112. Please see this policy for additional information.

Background - History on the creation of or changes to this policy

The NetWare Managers Group Policy Committee originally created this policy. The policy and 2002 revisions were reviewed with the Information Technology Managers Council for comment prior to adoption. The state information security committee made slight modifications to this policy in 2004

D. Guidelines - Recommendations, Not Requirements

Suspicious email messages should be forwarded to email address: virusreports@mt.gov for investigation before they are opened.

Users should write protect all diskettes whenever possible. A write-protected diskette cannot be infected unless there is a hardware error that disables the write protection. If the diskette requires write ability, it can be enabled at that time.

Users should not leave diskettes in the computer when not needed. A PC can become infected from a diskette left accidentally in a PC if the PC reboots due to an error or the power goes off momentarily. The PC will attempt to boot from the diskette in the drive. This can immediately infect the hard disk if a boot sector virus is present on the diskette, even if the boot process is not successful.

E. Change Control and Exceptions

Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this policy are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form. Changes to policies and standards will be prioritized and acted upon based on impact and need.

III. Close

For questions or comments about this instrument, contact the Information Technology Services Division at ITSD Service Desk, or:

Chief Information Officer
PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

IV. Cross-Reference Guide

A. State/Federal Laws

- 2-17-505(1) – Policy
- 2-17-514(1) – Enforcement
- §2-17-505(2), MCA
- §2-17-512, MCA
- §2-15-114, MCA

B. State Policies (IT Policies, MOM Policies, ARM Policies)

- 2-15-112, MCA
- 2-17-534, MCA
- 2-15-114, MCA
- 45-6-311, MCA
- MOM 1-0250.00
- ARM 2.13.101 - 2.13.107 - Regulation of Communication Facilities
- MOM 3-0130 Discipline
- ARM 2.12.206 Establishing Policies, Standards, Procedures and Guidelines.

C. IT Procedures or Guidelines Supporting this Policy

- Policy: Establishing and Implementing Statewide Information Technology Policies and Standards
- Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards

V. Administrative Use

Product ID:	ENT-SEC-102
Proponent:	Steve Bender, Acting Director, Department of Administration
Version:	1.1
Approved Date:	July 15, 2008
Effective Date:	October 2004
Change & Review Contact:	ITSD Service Desk
Review Criteria:	Event Review: Any event affecting this policy may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	July 1, 2013
Last Review/Revision:	Reviewed July 11, 2008. Non-material changes are necessary.
Change Record:	July 11, 2008 – Non-material changes made: - Standardize instrument format and common components. - Changed to reflect next review date.